REMARKS

RESPONSE TO 'EXAMINER'S RESPONSE TO AMENDMENT'

In the Office Action mailed November 26, 2007, at pages 2-4, the Examiner provided the following arguments/remarks (as numbered below) regarding the arguments provided by the Applicants in the Response dated September 4, 2007:

> 3. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Applicants' Response: Applicants respectfully disagree that their arguments "amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references." In accordance with what is stated in 37 CFR 1.111(b), the Applicants provided a reply to the Office Action dated June 1, 2007, addressing the supposed errors in the Examiner's action and replied to each and every ground of objection and rejection in this Office Action. The Response provided arguments believed to render the claims patentable over the applied references. Further, the Applicants provided "a *bona fide* attempt to advance the application to final action," as stated in 37 CFR 1.111(b). Thus, the Applicants respectfully submit that Applicants' argument complied with 37 CFR 1.111(b). Consequently, this rejection should be withdrawn.

> 4. Applicant's arguments do not comply with 37 CFR 1.111(c) because they do not clearly point out the patentable novelty which he or she

> thinks the claims present in view of the state of the art disclosed by the references cited or the objections made. Further, they do not show how the amendments avoid such references or objections.

Applicants' Response: Applicants clearly pointed out the patentable novelty in the claims in view of the state of the art disclosed by the references cited or the objections made. Applicants respectfully submit that Applicants' argument complied with 37 CFR 1.111(c). Absence a teaching of what is recited in the pending claims, the Applicants' respectfully submit that the rejection(s) should be withdrawn. Further, Applicants respectfully disagree with Examiner's remark that "Further, they do not show how the amendments avoid such references or objections," because the Applicants *did not* make any amendments to the original claims. Therefore, Applicants had no reason to "show how the amendments avoid such references or objections." Consequently, this rejection should be withdrawn.

> 5. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller,* 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Applicants' Response: Applicants' arguments pointed out that the references did not teach the claimed subject matter individually and in combination. In instances, where only one reference was used in a 35 U.S.C. 102 rejection, the arguments pointed out that the reference did not teach what was recited in the claims. In instances where more than a single reference was used to show a teaching of the claimed subject matter, Applicants respectfully submit that the

Applicants' intent is to show that the references in combination as well as individually do not teach what is recited in the claims. Consequently, this rejection should be withdrawn.

> 6. Examiner notes the absence of arguments or reply to the rejection of claim 1, as anticipated by Meiyappan (US Patent 6,993,542).

Applicants' Response: Applicants respectfully submits that Claim 1 is not anticipated by Meiyappan. In the Office Action of September 4, 2007, the Examiner had stated:

> Meiyappan discloses a method of generating pseudo-random numbers (col. 1 lines 65-col. 2 lines 2 and col. 1 lines 19-24) using a linear feedback shift register (fig. 1 element 112) in which the correlation between successive pseudo-random numbers is reduced (col. 1 lines 19-24 and abstract), said method comprising sampling output sequences of said linear feedback shift register with a specified periodicity (col. 3 lines 14-32 and fig. 2 element 206).

Applicants have thoroughly reviewed Meiyappan, at col. 1, lines 65-col. 2 lines 2 and col. 1 lines 19-24, at fig. 1 element 112, at col. 1 lines 19-24 and the abstract, at col. 3 lines 14-32, and at fig. 2 element 206; however, none of these passages teaches "sampling output sequences of said linear feedback shift register with a specified periodicity," as recited in Claim 1. As stated in Meiyappan, at col. 3, lines 16-21:

> At step 206, a sampling switch 110 samples the output of bit reordering block 108. Sampling switch 110 samples during periods when its sampling input line is active and does not sample when its sampling input is inactive. Sampling switch 110 may be implemented by a simple FET. The sampling input to sampling switch 110 is provided by the output of a linear feedback shift register 112.

Consequently, Meiyappan discloses that the sampling switch samples when its sampling input line is active as provided by the output of a linear feedback shift register. Nowhere does Meiyappan disclose anything about "sampling output sequences of a linear feedback shift register with a specified periodicity," as recited in Claim 1." Meiyappan simply discloses a linear feedback shift register output which is used to sample the output of a bit reordering block by way of a sampling switch. As an illustrative aid, the Examiner is requested to refer to Figure 1 of Meiyappan, which clearly supports what is described at col. 3, lines 16-21. Therefore, for these reasons, Meiyappan does not teach what is recited in Claim 1. Consequently, the Office Action does not show a teaching of what is recited in Claim 1. Applicant respectfully submits that Claim 1 contains patentable subject matter, which should be allowed.

> 7. Regarding Applicant's argument in reference to claim 1, the feature "a method of generating pseudo-random numbers using a linear feedback shift register in which the correlation between successive pseudo-random numbers is reduced", is taught because the "in which the correlation between successive pseudo-random numbers is reduced" is not a feature of the claim, but a result of the method by "sampling output sequences of said linear feedback shift register with a specified periodicity". This feature, namely "sampling output sequences of said linear feedback shift register with a specified periodicity" is taught in the reference by the cited paragraphs (0096, 0046, abstract, 0026-0027, and 0097), since the numbers are picked at specified clock periods. Therefore, since the method in the reference performs the claimed step, it inherently achieves the same result of "in which the correlation between successive pseudorandom numbers is reduced". **Applicant's arguments are not persuasive.**

Applicants' Response: Applicants have re-reviewed Gressel, at paragraphs 0096, 0046, 0026-0027, 0097, and at the abstract; however, Applicants do not see how Gressel teaches what is recited in Claim 1. For example, Applicants do not see how Gressel teaches "sampling output sequences of said linear feedback shift register with a specified periodicity," as recited in Claim 1. As supported and as described in the Applicants' specification, for example, at page 9 and at Figure 3, the Examiner should easily understand what is recited in Claim 1. Figure 3 illustrates the output of a 3-bit LFSR used in Figure 1 when it is sampled, for example, at every 3 iterations.

Applicants further note that the Examiner has characterized what is disclosed in Gressel when he alleges that "This feature, namely "sampling output sequences of said linear feedback shift register with a specified periodicity" is taught in the reference by the cited paragraphs (0096, 0046, abstract, 0026-0027, and 0097), *since the numbers are picked at specified clock periods*. (Examiner's characterization is denoted in italics). Nowhere does Gressel disclose "numbers" that "are picked at specified clock periods."

Instead, Gressel, at paragraph [0027] states:

> Conceptually, included in the embodiments of the generators described above are central processing units, CPUs, and finite state machines, FSMs. Finite state machines are logic control devices that typically control sequential processes. The FSMs typically assure that a programmer can only enhance or enable operation of the preferred embodiments. The CPU when programmed with secured immutable memory, with "frozen" methods of sampling typically ensures intractably computable correlation between the state of the number generating logic and the clock period of the sample. According to one preferred embodiment of the present invention, the FSM audits, "on the fly", the qualities of the random strings to ensure a more even histogram of words of the output strings.

The Applicants respectfully submits that this paragraph describes how a finite state machine is sampled using a CPU. For example, the passage states that "the CPU when programmed with secured immutable memory, with "frozen" methods of sampling typically ensures intractably computable correlation between the state of the number generating logic and the clock period of the sample." The preceding passage does not in any way teach "sampling output sequences of a linear feedback shift register with a specified periodicity," as recited in Claim 1. Thus, for at least this reason, the rejection to Claim 1 should be withdrawn.

Gressel, at the abstract, discloses:

> A microelectronic apparatus and method for generating random binary words including at least one clocked pseudorandom binary number sequence generator normally operative to generate a cyclic output sequence of binary numbers, each number including a string of binary symbols, the cyclic output sequence including a basic sequence which is generated repeatedly, at least one bit stream generator generating a clocked bit stream including a stream of binary symbols of a first type occasionally interrupted by a binary symbol of a second type, wherein a first varying time interval between the occasional interruptions is intractably correlated to the output sequence of the number sequence generator, wherein each occurrence of an interruption of the stream of binary symbols of the first type by a binary symbol of the second type causes a pseudorandom modification of the cyclic output sequence of the number sequence generator and a sampling device operative to sample the cyclic output sequence of binary numbers thereby to generate a sampled output sequence including at least one sampled binary word.

Nowhere does the abstract disclose anything about "sampling output sequences of a linear feedback shift register with a specified periodicity," as recited in Claim 1. Thus, for at least this reason, the rejection to Claim 1 should be withdrawn.

Gressel, at paragraph [0026], discloses that many mathematical functions "produce sequences, which pass all tests for randomness for almost all numerical inputs," and that "such functions are called pseudo-random." There is nothing in paragraph [0026] that teaches "sampling output sequences of a linear feedback shift register with a specified periodicity," as recited in Claim 1. Thus, for at least this reason, the rejection to Claim 1 should be withdrawn.

Gressel, at paragraph [0046] states:

> If an adversary or hacker knows 2^n (2 to the power of n) bits of a sequence of an unmodified n bit LFSR, he or she can easily derive the feedback configuration, which produced the sequence. If an oracle knows the configuration of an unmodified LFSR, and he/she can sample the contents of the device at a given clock cycle, if he/she can know the number of clock cycles that occurred before or after the known clock period, he/she can derive the contents at such given instant. All of the embodiments preferably have elements, which prevent the hacker from estimating the stage of the output at a given sampling, as all embodiments contain non-linear functionality derived from random sources.

Gressel, at paragraph [0046] teaches an unmodified n bit LFSR and how an adversary or hacker could derive the LFSR's feedback configuration. It also teaches that if an oracle knows the configuration of an unmodified LFSR, that he/she could sample the contents of the device (LFSR) at a given (single) clock cycle and derive the contents at the given instant, if he/she knows the number of clock cycles occurring before or after the known clock period. However, none of this verbiage teaches "sampling output sequences of a linear feedback shift register with a specified periodicity," as recited in Claim 1. Thus, for at least this reason, the rejection to Claim 1 should be withdrawn.

Gressel, at paragraph [0096] states:

> Also provided, in accordance with another preferred embodiment of the

> present invention, is apparatus for enhancing the randomness of an output binary stream, the apparatus including at least one random binary stream generator, and apparatus for generating an output binary stream by combining a plurality of n-bit samplings of the at least one random binary stream generated by the at least one random binary stream generator.

The preceding passage does not teach "sampling output sequences of a linear feedback shift register with a specified periodicity," as recited in Claim 1. It does not even teach "a linear feedback shift register," as recited in Claim 1. Thus, for at least this reason, the rejection to Claim 1 should be withdrawn.

Gressel, at paragraph [0097] states:

> Further in accordance with a preferred embodiment of the present invention, the apparatus for generating includes XOR apparatus for XORING the plurality of n-bit samplings.

The preceding passage teaches nothing about "sampling output sequences of a linear feedback shift register with a specified periodicity," as recited in Claim 1. Thus, for at least this reason, the rejection to Claim 1 should be withdrawn.

Applicants have thoroughly examined and reviewed the Examiner's cited passages in Gressel. However, none of these passages (i.e., Gressel, at paragraphs 0096, 0046, 0026-0027, and 0097, and at the abstract) teach what is recited in Claim 1. The Office Action has not shown a teaching of each and every element and/or feature recited in Claim 1. Therefore, Applicants respectfully submit that Claim 1 contains patentable subject matter. Applicants request allowance of independent Claim 1 and its associated dependent claims.

> 8. Regarding Applicant's argument in reference to claim 7, same argument as above applies to the alleged feature of "in which the correlation

between successive pseudo-random numbers is reduced".

Applicants' Response: In item #7 above, the Examiner had previously stated that "the feature "a method of generating pseudo-random numbers using a linear feedback shift register in which the correlation between successive pseudo-random numbers is reduced", is taught because the "in which the correlation between successive pseudo-random numbers is reduced" is not a feature of the claim, but a result of the method by "sampling output sequences of said linear feedback shift register with a specified periodicity"." In response, the Applicants direct the Examiner to the arguments provided in item #7 above, which show that the Office Actions do not show a teaching of "sampling output sequences of said linear feedback shift register with a specified periodicity," as recited in Claim 1. Consequently, the Examiner's argument of item #8 is ineffective and the Office Action does not show a teaching of "in which the correlation between successive pseudo-random numbers is reduced," as recited in Claim 1. Thus, for at least this reason, the Applicants respectfully submit that Claim 1 contains patentable subject matter. Consequently, the Applicants request allowance of independent Claim 1 and its associated dependent claims.

> 9. Regarding the step of "periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register" (col. 67 lines 36-col. 68 lines 2), Examiner respectfully submits that "this embodiment switches the connection of the switching circuit 1309 in response to the control signal after a predetermined number of bits are shifted in the LFSR 1302.", clearly anticipating "periodically switching", not after a time period per se, but after some action takes place. **Applicant's arguments are not persuasive.**

Applicants' Response: Furuta, at col. 67 lines 36-col. 68 lines 2, states:

> FIG. 126 shows an embodiment of the switching circuit 1309. This switching circuit 1309 includes an OR gate 1310, AND gates 1311 and 1312, and an inverter 1313 which are connected as shown. The control signal is input to the terminal 1314, and the bits b_0 and b_6 output from the output parts 1303 and 1304 of the flipflops 1302_1 and 1302_7 are respectively input to terminals 1317 and 1316. An output of the OR gate 1310 is output from a terminal 1318 and is supplied to the input part 1306 of the flip-flop 13021 as the output of the switching circuit 1309.
>
> Normally, the switching circuit 1309 selectively outputs the output of the exclusive-OR gate 1305 in response to the control signal. In this case, the connection of the random number generator 331 shown in FIG. 125 is the same as that shown in FIG. 74. But since the random pulses will be repeated periodically if this connection is fixed, this embodiment switches the connection of the switching circuit 1309 in response to the control signal after a predetermined number of bits are shifted in the LFSR 1302.
>
> For example, this predetermined number of bits corresponds to the number of bits which are shifted in the LFSR 1302 during one period of the random pulses. When the connection of the switching circuit 1309 is switched to selectively output the bit b6 from the flipflop 1302_7, the initial value set in the LFSR 1302 after one period of the random pulses is changed from the original initial value by shifting an arbitrary number of bits in the LFSR 1302. Thereafter, the connection of the switching circuit 1309 is returned to selectively output the output of the exclusive-OR gate 1305. Therefore, it is possible to guarantee the random nature of the random pulses over a plurality of periods of the random pulses.

While Furuta, at col. 67, lines 36 - col. 68, lines 2, may disclose an embodiment that "switches the connection of the switching circuitry 1309 in response to the control signal after a predetermined number of bits are shifted in the LFSR 1302," the Applicants respectfully submit that Furuta does not teach or disclose "periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register," as recited in Claim 7. Nowhere does Furuta disclose anything about "periodically switching," for example. Nor does Furuta disclose anything about periodically switching "between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register," as recited in Claim 7. Furthermore, Figure 126 of Furuta discloses only *one* linear feedback shift register. Thus, Furuta does not teach "iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register," as recited in Claim 7. Therefore, for at least these reasons, Furuta does not teach what is recited in Claim 7. The Office Action has not shown a teaching of what is recited in Claim 7. Therefore, the Applicants respectfully submit that Claim 7 contains patentable subject matter. Applicants request allowance of independent Claim 7 and its associated dependent claims.

> 10. Regarding Applicant's argument in reference to claim 11, Thomas clearly teaches the claimed subject matter, as follows, "operating a nonlinear operator on said pseudo-random number and one or more operands" (claim 29, and par. 0213, and 0155, the two taps map to the one or more operands). See also claim 29. **Applicant's arguments are not persuasive.**

Applicants' Response: Thomas, at Claim 29, states:

> 29. A system for securing communications channels, comprising:
> a register comprising;
> a first tap and a second tap for calculating a first value taken

> between the outputs of the first and second taps, the output between the first tap and second tap comprising a non-linear value;
>
> an output of the register taken between the first value and a third output bit of the register; and
>
> a new bit comprising an operation taken between the taps of the register.

Thomas, at paragraph 0155, states:

> Referring now to FIG. 10, this figure illustrates a submethod 905 for generating non-linear filtered output bits from shift registers. Step 1005 is the first step of the submethod 905 in which a first tap such as tap 735 and a second tap such as tap 740 of the linear feedback shift register 705 in FIG. 7 are selected. Next, a least significant output bit such as 730 is selected. Next, in Step 1015, the output of the first tap 735 and second tap 740 are combined.

Thomas, at paragraph 0213, states:

> The present invention has an increased encryption key size that reduces the possibility of a successful attack on a communications channel using the encryption key. The present invention also increases the speed at which a key stream is generated. The present invention generates a key stream that is not derived from shift registers possessing linear relationships between feedback taps. The present invention generates a key stream from feedback taps in a non-linear manner which prevents any attacks on the communication channel when the key stream is used to carry information between parties.

The Applicants do not see how Thomas, at Claim 29, paragraphs 0213 and 0155, could possibly be used to show a teaching of "operating a nonlinear operator on said pseudo-random number and one or more operands," as recited in Claim 11. The Examiner alleges that "the two taps map to the one or more operands." However, the Applicants respectfully disagree. Instead, Claim 29 discloses "a first tap and a second tap for calculating a first value taken between the output of the first and second taps." Thus, the first tap and second tap are simply used for calculating a first value, which is different from what is recited in Claim 11. Nowhere does Claim 29 disclose that the two taps correspond or map to one or more operands of a non-linear operator. Thus, based on what is disclosed in Thomas, the Applicants respectfully believe that the Examiner has improperly characterized what is disclosed in Thomas, when he alleges "the two taps map to the one or more operands." Further, the Applicants respectfully submit that Thomas, at paragraph 0155 merely discloses that a first tap and a second tap of a linear feedback shift register are selected while Thomas, at paragraph 0213 does not provide a teaching of any element recited in Claim 11.

In addition, the Examiner does not show "operating a nonlinear operator" on a "psuedo-random number *and* one or more operands," as recited in Claim 11. Thomas, at paragraph 0155 or at paragraph 0213, or at Claim 29 does not teach one or more operands *and* a pseudo-random number being operated on by a nonlinear operator (emphasis denoted in italics). Thus Thomas does not teach what is recited in Claim 11.

Therefore, for at least the foregoing reasons, the Office Action does not show a teaching of each and every element and/or feature recited in Claim 11. Therefore, Claim 11 contains patenable subject matter, and Claim 11 should be allowed. Applicants request allowance of independent Claim 11 and its associated dependent claims.

> 11. Regarding Applicant's argument in reference to claim 17, Walmsley clearly teaches "varying the initial value of said hashing function over

> time by way of a function operating on one or more variables" (0358-0365 and 0942-0943, the use of time varying random number is encrypted for the signature - hash). **Applicant's arguments are not persuasive.**

Applicants' Response: The Examiner contends that Walmsley, at paragraphs 0358-0365 and paragraphs 0942-0943 teaches "A method of further encrypting a pseudo-random number generated from a linear feedback shift register by using a hashing function comprising: receiving said pseudo-random number generated from said linear feedback shift register; and varying the initial value of said hashing function over time by way of a function operating on one or more variables," as recited in Claim 17. The Examiner has stated that "the use of time varying random number is encrypted for the signature – hash." The Examiner appears to be referring to Walmsley, at paragraph 0360, which states:

> The secret keys are not revealed during the authentication process. The time varying random number is encrypted, so that it is not revealed during the authentication process.

The preceding paragraph does not teach an "initial value of said hashing function over time," as recited in Claim 17. Nowhere in Walmsley, at paragraph 0360, is there any disclosure of an initial value of a hashing function as recited in Claim 17. Thomas, at paragraph 0360, discloses a time varying random number; however, nowhere does Thomas teach that this time varying random number is an initial value of a hashing function. Therefore, for at least this reason alone, Walmsley does not teach what is recited in Claim 17. Furthermore, the Office Action does not show a teaching of a "function operating on one or more variables," as recited in Claim 17. Therefore, for at least this reason alone, Claim 17 is in condition for allowance. Applicants request allowance of independent Claim 17 and its associated dependent claims.

Based on at least the foregoing arguments for independent Claims 1, 7, 11, and 17, the Applicants respectfully submit that the pending claims are in condition for allowance. Therefore, the Applicants request the Examiner to advance the pending claims to allowance.

APPLICANTS' RESPONSE TO CLAIM REJECTIONS - 35 U.S.C. § 102(E) AND 35 U.S.C. § 103(A) (PAGES 4-8 OF FINAL OFFICE ACTION)

With regard to the rejections for the pending claims, as presented in the final Office Action, at pages 4-8, the Examiner has restated exactly the same remarks/arguments that were made in the non-final Office Action mailed on June 1, 2007. Therefore, the Applicants request the Examiner to refer to Applicants' Response, dated September 4, 2007. The Applicants stand by the arguments provided in this Response. Furthermore, the Applicants maintain that the pending claims are allowable for at least the reasons stated in the current Response, as detailed in the section, RESPONSE TO 'EXAMINER'S RESPONSE TO AMENDMENT'.

Consequently, the Applicants respectfully submit that the pending claims should be advanced to allowance.

CONCLUSION

Based on at least the foregoing, the Applicants believe that Claims 1-22 are in condition for allowance. A Notice of Allowance is courteously solicited. Should anything remain in order to place the present Application in condition for allowance, or should the Examiner disagree or have any question regarding this submission, the Examiner is kindly invited to contact the undersigned at (312) 775-8246.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the Deposit Account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Dated: January 28, 2008

Respectfully submitted,

/Roy B. Rhee/

Roy B. Rhee
Reg. No. 57,303

McAndrews, Held & Malloy, Ltd.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661-2565
Telephone: (312) 775-8246
Facsimile: (312) 775-8100